

Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of)	
)	
Implementation of the Telecommunications Act of 1996)	CC Docket No. 96-115
)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information;)	
)	
Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended)	CC Docket No. 96-149
)	

**REPLY COMMENTS OF
THE INTELLIGENT TRANSPORTATION
SOCIETY OF AMERICA**

Jason M. Conley
Deputy General Counsel
Intelligent Transportation Society
Of America
400 Virginia Avenue, SW
Suite 800
Washington, DC 20024
(202) 484-4847

Robert B. Kelly
Mark D. Johnson
Squire, Sanders & Dempsey L.L.P.
1201 Pennsylvania Avenue, N.W.
P.O. Box 407
Washington, D.C. 20044-0407
(202) 626-6600

Its Attorneys

November 16, 2001

Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of)	
)	
Implementation of the Telecommunications Act of 1996)	CC Docket No. 96-115
)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information;)	
)	
Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended)	CC Docket No. 96-149
)	

To: The Commission

**REPLY COMMENTS OF
THE INTELLIGENT TRANSPORTATION
SOCIETY OF AMERICA**

The Intelligent Transportation Society of America ("ITS America"), by its attorneys and pursuant to Section 1.415 of the Commission's rules, 47 C.F.R. § 1.415, respectfully submits its Reply Comments addressing comments filed in response to the Clarification Order and Second Further Notice of Proposed Rulemaking ("2d FNPRM") in the above-captioned proceedings¹ regarding the use and disclosure of Customer Proprietary Network Information ("CPNI") by telecommunications carriers.

¹ *In the Matter of Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Standards of Sections 271 and 272 of the Communications Act of 1934, As Amended*, CC Dockets Nos. 96-115 and 96-149, Clarification Order and Second Further Notice of Proposed Rulemaking, FCC 01-247 (rel. September 7, 2001) ("2d FNPRM").

In this proceeding, the Commission has asked for comments regarding what rules the Commission should adopt for implementing Section 222 of the Communications Act, as amended,² to govern the use and disclosure of CPNI by telecommunications carriers. ITS America's Reply Comments are limited to the Commission's inquiry on the use and disclosure of wireless call location information that is now considered CPNI under Section 222.³ ITS America agrees with those commenters who request that the Commission address this issue within a separate rulemaking proceeding initiated earlier this year.

I. INTRODUCTION

ITS America is a 501(c)(3), non-profit education and scientific research organization created in 1991 for the purpose of fostering the development and deployment of intelligent transportation systems⁴ throughout the United States. The organization is a unique public/private partnership, serving as a utilized Federal Advisory Committee to the U.S. Department of Transportation. Approximately half of ITS America's membership is comprised of public sector institutions such as state departments of transportation, metropolitan planning organizations, universities and other non-profit organizations. The other half of its members are from the private sector and

² 47 U.S.C. § 222.

³ *2d FNPRM* at ¶ 12.

⁴ Intelligent Transportation Systems ("ITS") represent the integrated application of advanced information, electronics, communications and other technologies to surface transportation systems. This includes freeway monitoring and incident management, and transit fleet management as well as traveler information systems. ITS technologies also include electronic payment systems such as smart cards and other toll-tag transponders. In-vehicle electronic systems such as GPS-based navigation systems, automated crash notification, and collision avoidance systems are also ITS technologies.

include, among others, automobile manufacturers and suppliers, engineering firms, software designers, and telematics providers.

II. WIRELESS LOCATION INFORMATION

Customer Proprietary Network Information (“CPNI”) is information telecommunications carriers, landline and wireless, collect about their customers in order to provide the requested telecommunications service.⁵ Carriers are obligated to protect the confidentiality of CPNI.⁶ In 1999, the CPNI provisions were amended to include the location information of a wireless caller within the definition of CPNI and, accordingly, make this information subject to these same confidentiality protections.⁷ Section 222(f) was amended to read that: “[f]or purposes of [Section 222(c)(1)], without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to ... call location information concerning the user of a commercial mobile service” except in specified emergency situations.⁸ The Commission asks in the instant proceeding for comments regarding how the Commission should apply the confidentiality requirements imposed on carriers for CPNI in Section 222(c)(1) to call location information available from commercial wireless carriers.⁹

⁵ 47 U.S.C. § 222(g). CPNI includes the quantity, technical configuration, type, destination, location and the amount of use of a telecommunications service requested by a customer. *Id.*

⁶ 47 U.S.C. § 222(c)(1).

⁷ Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, 113 Stat. 1286 (1999) (relevant provisions codified in 47 U.S.C. § 222(f) & (g)).

⁸ 47 U.S.C. § 222(f).

⁹ 2d FNPRM at ¶ 22.

ITS America agrees with those commenters that ask that the Commission address this precise question in a separate proceeding currently underway.¹⁰ In late 2000, the Cellular Telecommunications & Internet Association (“CTIA”) filed a Petition for Rulemaking (“*CTIA Petition*”) asking that the Commission establish a set of Fair Location Information Practices applicable to wireless carriers.¹¹ In March of this year, the Commission put the *CTIA Petition* on public notice and requested comments on whether the requested rulemaking proceeding should be initiated.¹² To date, the Commission has yet to decide whether or not to issue a Notice of Proposed Rulemaking.

ITS America filed Reply Comments generally supporting the *CTIA Petition*, a copy of which is attached hereto as Appendix A.¹³ In addition to submitting its own set of Fair Information and Privacy Principles for the Commission to consider, ITS America supported CTIA’s request that a separate rulemaking proceeding be initiated to address the issue of what privacy and disclosure protections should be applied to wireless call

¹⁰ Comments of ALLTEL at 6-7; Comments of Sprint Corporation at 7-8; Comments of Cingular Wireless at 8-10; Comments of the Cellular Telecommunications & Internet Association at 6.

¹¹ See *In the Matter of Petition for Rulemaking* Petition of the Cellular Telecommunications & Industry Association for a Rulemaking to Establish Fair Location Information Practices (submitted November 22, 2000) (“*CTIA Petition*”)

¹² *Wireless Telecommunications Bureau Seeks Comment on Request to Commence Rulemaking to Establish Fair Location Information Practices*, Public Notice, DA 01-696 (rel. March 16, 2001). The Commission assigned WT Docket No. 01-72 to identify the proceeding.

¹³ See *In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles*, WT Docket No. 01-72, Reply Comments of the Intelligent Transportation Society of America (submitted April 24, 2001) (“*ITS America Reply Comments*”). ITS America asks that these comments be incorporated by reference in the instant proceeding.

location information.¹⁴ ITS America herein reiterates its support for a separate rulemaking proceeding.

While the instant proceeding is also concerned with how carriers may use and disclose CPNI, the issues associated with wireless call location information vary significantly. Accessing wireless location call information utilizes different technologies, may be employed for different purposes and carries with it far different privacy concerns than CPNI collected by landline carriers. As noted above, the underlying statutory predicate governing wireless call location information is not the same as for landline CPNI. In order to ensure the full and complete consideration of the privacy protections needed for wireless call location information, ITS America respectfully requests that the Commission address these questions in its current proceeding on the *CTIA Petition* in WT Docket No. 01-72.

III. REGULATING TELEMATICS PROVIDERS

If the Commission ultimately decides to consider wireless call location information in the instant proceeding, ITS America urges the Commission to refrain from applying its CPNI rules to telematics providers. The Commission lacks clear jurisdiction over this industry. Moreover, the market for telematics is still nascent and its development undetermined. Imposing regulations now would risk stifling the industry as it takes its first steps.

Telematics is a general term for the provisioning of a variety of safety, security and information services now available principally in passenger vehicles. With over one million cars currently equipped, General Motors' OnStar is probably the largest and best-

¹⁴ ITS America Reply Comments at 3.

known example. Telematics services utilize an analog wireless connection, provided in partnership with several national wireless carriers, to offer turn-by-turn directions, news and other information, as well as “mayday” assistance in case of an accident or other emergency.

ITS America agrees with the position of ATX Technologies, Inc. that the Commission cannot and should not apply its CPNI rules to telematics providers.¹⁵ First, Section 222 and its CPNI rules are clearly limited to telecommunications common carriers.¹⁶ While they employ a telecommunications link as part of their service offering, telematics providers are not typically in the business of offering to the public a telecommunications service for compensation.¹⁷ Telematics services are provided to subscribers who pay a monthly fee. The communications link from the vehicle to the telematics call center is made available by several of the national wireless carriers, not the telematics providers themselves. To this extent, telematics providers do not qualify as “common carriers” and, therefore, are not subject to the provisions of Section 222. In sum, Section 222 does not grant the Commission jurisdiction over telematics providers.

Second, telematics providers do not collect CPNI about their subscribers. In particular, the location of telematics subscribers is not determined through wireless Enhanced 911 technologies, whether handset or network based, but by a GPS device that is installed in the vehicle. Section 222’s provisions do not speak to GPS devices that are

¹⁵ Comments of ATX Technologies at 6-7.

¹⁶ See 47 U.S.C. § 222(a) (“Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of ... customers.”)

¹⁷ 47 U.S.C. § 153(10).

not within a handset or wireless network, nor is such location information a byproduct or derivative of any telecommunications service.

Finally, from a policy standpoint, ITS America cautions the Commission not to impose any regulations that could stifle this industry at its very formation. Telematics services have been available for less than five years. In addition, the types of services and products, and their market price points, remain undetermined. The Commission should therefore forgo imposing its CPNI rules on telematics providers. A more thorough review of this discrete issue could also be better conducted within the separate proceeding on *CTIA's Petition* in WT Docket No. 01-72.

IV. CONCLUSION

ITS America again urges the Commission to consider the application of its CPNI rules to wireless call location information as part of WT Docket No. 01-72. The Commission's statutory authority to regulate this type of information comes from a different statutory predicate. The underlying technologies, purposes and privacy implications are also different. ITS America also contends that the Commission lacks the

basis to apply the CPNI rules to telematics providers, both as a matter of law but also as a matter of sound public policy.

Respectfully submitted,

THE INTELLIGENT TRANSPORTATION
SOCIETY OF AMERICA

By: /s/ Robert B. Kelly

Jason M. Conley
Deputy General Counsel
Intelligent Transportation Society
Of America
400 Virginia Avenue, SW
Suite 800
Washington, DC 20024
(202) 484-4847

Robert B. Kelly
Mark D. Johnson
Squire, Sanders & Dempsey L.L.P.
1201 Pennsylvania Avenue, N.W.
P.O. Box 407
Washington, D.C. 20044-0407
(202) 626-6600

Its Attorneys

November 16, 2001

Appendix A

WT Docket No. 01-72

**Reply Comments of the Intelligent Transportation
Society of America (submitted April 24, 2001)**

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

RECEIVED

APR 24 2001

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles

WT Docket No. 01-72

REPLY COMMENTS OF THE INTELLIGENT
TRANSPORTATION SOCIETY OF AMERICA

Pursuant to the Commission's Public Notice, released March 16, 2001,¹ the Intelligent Transportation Society of America ("ITS America") hereby submits its Reply Comments in support of the of the petition of the Cellular Telecommunications and Internet Association ("CTIA") requesting a rulemaking proceeding to adopt proposed location information privacy principles.

I. Summary

ITS America agrees with CTIA that the Commission should initiate a separate rulemaking proceeding, distinct from the Commission's Customer Proprietary Network Information ("CPNI") docket, to address the location privacy issues raised by CTIA's petition. Moreover, ITS America respectfully agrees with those commenters who urge the Commission to state unequivocally that the collection and use of anonymous and aggregate location data by wireless carriers is not subject to CPNI restrictions. Aggregate information is explicitly excepted from CPNI as it is defined in Section 222 of the Telecommunications Act of 1996. Anonymous, non-personally identifiable location information collected by wireless carriers and delivered to traffic management centers for purposes of monitoring vehicle traffic flows should be considered to be aggregate

¹ *Wireless Telecommunications Bureau Seeks Comment on Request to Commence Rulemaking to Establish Fair Location Information Practices*, Public Notice, DA 01-696 (rel. March 16, 2001).

information for purposes of Section 222 and for any rulemaking proceeding considered by the Commission.

Recognizing the sensitivity of location information, ITS America has developed self-regulatory principles for the intelligent transportation community. These principles contain notice and consent provisions for the collection and use of personally identifiable information and an opt-out standard for the collection of non-personally identifiable information.

II. Statement of Interest

The Intelligent Transportation Society of America ("ITS America")² is a 501(c)(3) educational and scientific research organization created in 1991 for the purpose of fostering the development and deployment of intelligent transportation systems.³ ITS America is a unique public/private partnership, serving as a utilized Federal Advisory Committee to the U.S. Department of Transportation. Half of ITS America's membership is comprised of public sector institutions such as state departments of transportation, metropolitan planning organizations, universities and other non-profit organizations. The other half of its members are from the private sector.

² ITS America is organized to be the focal point for facilitating the consensus necessary to develop and deploy ITS technologies. The Society operates under the executive leadership of a 48 member board of directors comprised of executives of public and private organizations including the Deputy Secretary of U.S. Department of Transportation and other department executives and industry leaders from the world of ITS. Members include organizations that develop, deploy, market, research, buy, sell and use ITS products, services and systems. Members come from the private sector, local, state, federal and international government agencies, academic institutions and research centers, and other associations.

³ Intelligent Transportation Systems ("ITS") represents the integrated application of advanced information, electronics, communications, and other technologies to surface transportation systems. This includes freeway monitoring and incident management, and transit fleet management as well as traveler information systems. ITS technologies also include electronic payment systems such as smart cards and other toll-tag transponders. In-vehicle electronic systems such as GPS-based navigation systems, automated crash notification, and collision avoidance systems are also ITS technologies.

III. The Petition

ITS America agrees with CTIA's petition⁴ that the Commission should initiate a proceeding that is separate and distinct from the Commission's CPNI docket. There is, at present, substantial uncertainty regarding the requirements placed on a carrier's ability to market customer location information to secondary users of that data. This includes the provision of such data necessary to effectuate the goals of intelligent transportation. These goals include public benefits such as monitoring traffic flows to relieve roadway congestion, the delivery of traveler information to inform and empower individual drivers as to route selection, and the provision of "mayday" emergency response services.

The Wireless Communications and Public Safety Act of 1999 ("WCPSA")⁵ first determined that location information about the carriers' customers fell under the definition of Customer Proprietary Network Information ("CPNI").⁶ Second, the WCPSA required carriers to obtain a customer's "express prior authorization" before disclosing that customer's location information to third parties except in an emergency.⁷ Upon the written request of their subscribers, carriers must also disclose location information to third parties designated by their subscribers.⁸ As noted in the petition, the Commission has to date deferred implementing the location privacy provisions of the WCPSA. However, the Commission should act now to provide certainty to carriers and secondary users engaged in the deployment of intelligent transportation systems.

⁴ *In the Matter of Petition for Rulemaking*, Petition of the Cellular Telecommunications Industry Association for a Rulemaking to Establish Fair Location Information Practices (submitted November 22, 2000) ("*CTIA Petition*").

⁵ Pub. L. No. 106-81, 113 Stat. 1286 (1999) (codified at 47 U.S.C. § 222).

⁶ 47 U.S.C. § 222(h)(1)(A).

⁷ *Id.* at § 222(f)(1).

⁸ *Id.* at § 222(c)(2).

IV. Initial Comments Regarding CTIA's Petition

Twenty-four initial comments were submitted, the majority of which supported CTIA's petition. Supporting comments were received from wireless carriers,⁹ equipment manufacturers,¹⁰ industry associations,¹¹ an application provider¹² and the 911 community.¹³ Two public interest organizations expressed strong support behind the establishment of location information privacy principles.¹⁴ This issue, however, is not without controversy. Several commenters noted their belief that industry self-regulation would be more effective in protecting an individual's location information than would any government regulations.¹⁵ Still other commenters agree that location information should be protected, but question whether a formal rulemaking is appropriate at this time and if CTIA's proposed principles are workable.¹⁶

V. Any Rulemaking Should be Technologically Neutral

ITS America agrees with CTIA's proposed privacy principle that any restrictions on the collection and use of location data be technologically neutral. Several supporters

⁹ Comments of Cingular; Comments of Dobson Communications Corporation; Leap Wireless; Sprint PCS.

¹⁰ Comments of Ericsson; Comments of Nokia.

¹¹ Comments of Location Privacy Association; Comments of Rural Telecommunications Group; Comments of Wireless Location Industry Association; Comments of XNS Public Trust Organization.

¹² Comments of SiRF Technology.

¹³ Comments of Texas 911 Agencies.

¹⁴ Comments of Center for Democracy and Technology; Comments of Electronic Privacy Information Center.

¹⁵ Comments of Direct Marketing Association; Comments of Wireless Advertising Association.

¹⁶ Comments of AT&T Wireless; Comments of TruePosition, Inc.; Comments of Verizon Wireless; Comments of Wireless Consumers Alliance.

of CTIA's petition also concur that any rules promulgated by the Commission should not favor one technology over another.¹⁷

The Commission should realize, however, that other non-carriers also have the ability to collect location data. Closed circuit cameras, loop detectors, and transponders used by electronic toll collection systems have the capability to track the location of a vehicle as it travels through a metropolitan area. Parties utilizing these other methods of location data collection also have the ability to aggregate and distribute vehicle location data. However, each of these data collection methods complements rather than substitutes the location data collected by wireless carriers. A rich diversity of data feeds is necessary to ensure that accurate and effective intelligent transportation systems continue to mitigate congestion.

The WCPPA applies only to telecommunications carriers.¹⁸ However, it is not clear whether these same obligations to protect privacy would also apply to non-carriers. The Commission should recognize that there might be non-carriers involved in the collection of personally identifiable information, including location information. Consequently, the Commission should consider whether there is a need to extend WCPPA's privacy protections to these non-carriers and whether it has a proper basis to exercise its jurisdiction over them.

VI. The Use of Anonymous Location Data Should Not Be Impeded

The collection of anonymous, non-personally identifiable location data should not be subject to notice and consent requirements. CTIA's petition acknowledges as much, noting that under the CPNI framework, "a telecommunications carrier may, without customer approval, use, disclose or permit access to aggregate customer information

¹⁷ Comments of Dobson Communications Group at 5; Comments of Ericsson at 3; Comments of Leap Wireless at 7; Comments of Nokia at 5 Comments of Rural Telecommunications Group at 4.

¹⁸ See 47 U.S.C. § 222(c) (Each telecommunications carrier has a duty to maintain the confidentiality of CPNI information, including location information, related to their customers.)

that contains location information from which individual customer identities and characteristics have been removed.”¹⁹ This is the so-called “aggregate information” exception to the CPNI confidentiality restrictions on carriers.²⁰ To ensure the continued use of aggregate location information in intelligent transportation systems, ITS America urges the Commission to explicitly state that the collection and use of non-personally identifiable location data enjoys the exemptions of other aggregate information.²¹

Two types of anonymous location data are utilized in intelligent transportation systems. Traffic management centers and traffic information service providers often rely on “anonymous aggregate” location information.²² In this form of collection, carriers track the location of wireless customers, strip this information of personal identifiers, and aggregate the data before delivering it to secondary users. Traffic management centers use this information about the approximate location of wireless telephone users in automobiles to provide the general public, emergency services, and professional traffic managers with reliable and accurate traffic flow information.

When the signal of a wireless customer is tracked, stripped of personal identifiers, but not aggregated with the location of other customers, the result is referred

¹⁹ *CTIA Petition* at 6-7.

²⁰ See 47 U.S.C. § 222(c)(3) (permitted carriers to disclose “aggregate customer information” to third parties without the consent of the customer). “Aggregate Information” is defined elsewhere in the CPNI provisions as “collective data that relates to a group or category of services or customers, from which individual customer identifies and characteristics have been removed.” *Id.* at § 222(h)(2).

²¹ One commenter, the Wireless Location Industry Association, also noted the importance of maintaining the availability of aggregate information for a variety of purposes, including for traffic management purposes. Comments of Wireless Location Industry Association at 6.

²² Traffic management centers use remote video cameras at key points on high-traffic roadways, to observe highway traffic conditions in real-time. Traffic engineers at these centers compile traffic information gathered through several sources, including aggregated data feeds of the location and movement of wireless telephone users, closed circuit television cameras, remote sensing platforms, and sensors embedded in the roadways. This information is used to promote the free-flow of traffic, enable the timely dispatch of emergency services, and to provide the traveling public with accurate traffic information.

to as "origin-destination" information. Collection of this type of data has the potential to provide traffic engineers and planners with rich data feeds, necessary to promote optimal traffic flows, efficiently allocate transportation resources, and to properly reroute traffic in emergency situations. "Origin-destination" information is a necessary component to intelligent transportation and should not be subject to prior notice and consent restrictions.

VII. ITS America's Privacy Principles for Intelligent Transportation Systems

ITS America has been proactive in addressing the sensitive issue of location privacy. In July 10, 1996, ITS America drafted the "Interim Intelligent Transportation Systems (ITS) Fair Information and Privacy Principles" in recognition of the importance of protecting individual privacy in implementing Intelligent Transportation Systems. The ITS principles represent values and are designed to be flexible and durable to accommodate a broad scope of technological, social and cultural change. These principles were created to advise ITS America members, committees and board of directors, and are intended to educate and guide transportation professionals, policy makers, and the public as they develop fair information and privacy guidelines for specific ITS projects.

Fulfilling its public purpose as a 501(c)(3) organization, ITS America sought and considered the input of consumers, law enforcement, industry, government, and privacy advocates in the final version of its Privacy Principles. After four years of consideration and amendment, ITS America's Board of Directors approved these principles on January 11, 2001 as voluntary guidance for the intelligent transportation community. A copy of the final Privacy Principles are attached as Appendix A.

ITS America agrees in principle with the privacy framework established in CTIA's petition, (a self-regulatory regime based on the principles of notice, consent, integrity,

and technological neutrality). However, ITS America believes that its own privacy principles are better tailored to meet the needs of the intelligent transportation community.²³ The principles apply equally to all technologies capable of collecting location data. Moreover, they provide an "opt-out" regime for the use of anonymous, non-personally identifiable location data and an "opt-in" regime for the use of personally identifiable location data. This fine distinction, absent from CTIA's proposed privacy principles, is necessary to balance the public's interest in location privacy with the needs of traffic management centers use anonymous location data in monitoring traffic flows. Finally, the principles distinguish between location data collected and used for intelligent transportation purposes and that data used for secondary purposes. ITS America respectfully urges the Commission to consider ITS America's Privacy Principles during the course of any rulemaking proceeding respecting location information privacy.

VIII. Conclusion

Intelligent transportation systems utilize wireless location data to monitor traffic flows, reduce congestion, and to enable the provision of public services such as emergency response and traveler information. ITS America supports CTIA's petition for a separate proceeding to address the use of location data by wireless carriers. ITS America, in principle, supports the privacy framework described in CTIA's petition. However, ITS America strongly urges the Commission to provide an exception for the use of anonymous location data as well as aggregate location data. While recognizing

²³ See Attachment A.

the importance of location privacy, ITS America could only support a rulemaking that would not hinder the development and deployment of intelligent transportation systems.

Respectfully Submitted,

**The Intelligent Transportation Society of
America**

By:



Jason M. Conley, Esq.
Staff Counsel

Intelligent Transportation Society of
America
400 Virginia Avenue, SW
Suite 800
Washington, DC 20024
(202) 484-4847
(202) 484-3483 (fax)

CERTIFICATE OF SERVICE

I, Mark D. Johnson, hereby certify on this 24th day of April, 2001, I caused copies of the foregoing "Reply Comments of the Intelligent Transportation Systems of America" to be delivered to the following by either first-class mail, postage prepaid, or by hand (*):

Barbara Reideler*
Policy Division
Wireless Telecommunications Bureau
Room 3-B101
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Barbara A. Baffer
Director, Regulatory Affairs
Ericsson Inc.
Office of Public Affairs
1634 I Street, NW
Suite 600
Washington, DC 20006

International Transcription Service*
CY-B400
Federal Communications Commission
445 12 Street, SW
Washington, DC 20554

James H. Barker, Esq.
Latham & Watkins
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004

Michael Altschul
Vice President and General Counsel
Cellular Telecommunications & Internet
Association
1250 Connecticut Avenue, NW
Suite 800
Washington, DC 20036

James Green, Esq.
Executive Director
Tongour Simpson Holsclaw Green, LLC
227 Massachusetts Avenue, NE
Suite #1
Washington, DC 20002

J.R. Carbonell
Cingular Wireless, LLC
5565 Glenridge Connector
Suite 1700
Atlanta, GA 30342

Leo R. Fitzsimon
Director of Regulatory &
Industry Affairs
Nokia Inc.
1101 Connecticut Ave., NW
Washington, DC 20036

Ronald L. Ripley
Senior Corporate Counsel
Dobson Communications
13439 N. Broadway Est., Suite 200
Oklahoma City, OK 73114

Caressa Bennet, General Counsel
Rural Telecommunications Group
Bennet & Bennet, PLLC
1000 Vermont Avenue, NW
Tenth Floor
Washington, DC 20005

David Sobel
General Counsel
Electronic Privacy Information Center
1718 Connecticut Avenue, NW
Suite 200
Washington, DC 20009

Scott J. Rafferty
Senior Director, Business Development
SiRF Technology, Inc.
148 East Brokaw Road
San Jose, CA 95112

Luisa L. Lancetti
Vice President, PCS Regulatory Affairs
401 9th Street, NW
Suite 400
Washington, DC 20004

Rupaco T. Gonzalez, Jr., Esq.
The Gonzalez Law Firm, PC
One Westlake Plaza, Suite 100
1705 South Capitol of Texas Highway
Austin, TX 78746

Philip L. Verveer, Esq.
Willkie Farr & Gallagher
Three Lafayette Centre
1155 21st Street, NW
Suite 600
Washington, DC 20036

John T. Scott, III
Vice President and Deputy General
Counsel – Regulatory Law
Verizon Wireless
1300 I Street, NW
Suite 400 West
Washington, DC 20005


Robert O'Hare
Chairman of the Board
Wireless Advertising Association
38 Tyler Circle
Rye, NY 10580

Carl Hilliard
Wireless Consumers Alliance, Inc.
1246 Stratford Court
Del Mar, CA 92014

John W. Jimison, Esq.
Executive Director and General Counsel
Wireless Location Industry Association
1225 19th Street, NW
Suite 800
Washington, DC 20036

Ian D. Volner
Venable, Baetjer, Howard &
Civiletti, LLP
1201 New York Avenue, NW
Suite 1000
Washington, DC 20005

James X. Dempsey
The Center for Democracy &
Technology
1634 Eye Street, NW Suite 1100
Washington, DC 20006


Mark D. Johnson

APPENDIX A



INTELLIGENT TRANSPORTATION SOCIETY OF AMERICA

400 Virginia Ave., S.W., Suite 800
Washington, D.C. 20024-2730
(202) 484-4847 • FAX (202) 484-3483
<http://www.itsa.org>

ITS America's Intelligent Transportation Systems Fair Information and Privacy Principles

These fair information and privacy principles were prepared in recognition of the importance of upholding individual privacy in implementing Intelligent Transportation Systems (ITS). The principles represent values and are designed to be flexible and durable to accommodate a broad scope of technological, social and cultural change. ITS America may, however, need to revisit them periodically to assure their applicability and effectiveness.

These principles are advisory, intended to educate and guide transportation professionals, policy makers, companies, organizations, and the public as they develop fair information and privacy guidelines for specific intelligent transportation projects. Initiators of ITS projects are urged to publish the fair information and privacy principles that they intend to follow. Parties to ITS are urged to include enforceable provisions for safeguarding privacy in their contracts and agreements.

1. INDIVIDUAL CENTERED. Intelligent Transportation Systems must recognize and respect the individual's interests in privacy and information use.

ITS Systems create value for both individuals and society as a whole. Central to the ITS vision is the creation of ITS Systems that will fulfill our national goals. The primacy focus of information use is to improve travelers' safety and security, reduce travel times, enhance individuals' ability to deal with highway disruptions and improve air quality. Travel information is collected from many sources, some from the infrastructure and some from vehicles, while other information may come from the transactions -- such as electronic toll collection -- that involve interaction between the infrastructure and vehicle. That information may have value in both ITS and non-ITS applications. The individual's interest in privacy must be respected. This requires disclosure and the opportunity for individuals to express choice if personal identification is collected.

2. VISIBLE. Intelligent Transportation Information Systems will be built in a manner "visible" to individuals.

ITS may create data on individuals. Individuals should have a means of discovering how the data flows operate. "Visible" means to disclose to the public the type of data collected, how it is collected, what its uses are, and how it will be distributed. The concept of visibility is one of central concern to the public, and, consequently, this principle requires assigning responsibility for disclosure.

3. COMPLY. Intelligent Transportation Systems will comply with applicable state and federal laws governing privacy and information use.

Privacy law is a patchwork of federal and state statutes, as well as federal and state judicial opinions. The

“right” to privacy as a matter of law in the context of transportation on public roads and other facilities is limited. Intelligent Transportation Systems should provide, at a minimum, privacy protections in conformity with the law of respective jurisdictions.

4. SECURE. Intelligent Transportation Systems will be secure.

ITS databases may contain information on where travelers go, the routes they use, and when they travel, and therefore must be secure. All ITS information systems will make use of data security technology and audit procedures appropriate to the sensitivity of the information. ITS systems should use technological and administrative safeguards to assure that access to personally identifiable information is restricted to duly authorized individuals.

5. LAW ENFORCEMENT. Intelligent Transportation Systems have an appropriate role in enhancing travelers' safety and security interests, but absent consent, statutory authority, appropriate legal process, or emergency circumstances as defined by law, information identifying individuals will not be disclosed to law enforcement.

ITS has the potential to make it possible for traffic management agencies to know where individuals travel, what routes they take, and travel duration. Therefore, ITS can increase the efficiency of traffic law enforcement by providing aggregate information necessary to target resources. States may legislate conditions under which ITS information will be made available to law enforcement agencies. Absent government authority, however, ITS systems should not be used as a surveillance means for enforcing traffic laws, nor used as a tool of criminal investigation. Although individuals are concerned about public safety, persons who voluntarily participate in ITS programs or purchase ITS products should be informed of how information they are providing is used.

6. RELEVANT. Intelligent Transportation Systems will only collect personal information that is relevant for ITS purposes.

ITS, respectful of the individual's interest in privacy, will only collect information that contain individual identifiers that are needed for the ITS service functions. Furthermore, ITS information systems will include protocols that call for the purging of individual identifier information that is no longer needed to meet ITS needs.

7. ANONYMITY. Where practicable, individuals should have the ability to utilize Intelligent Transportation Systems on an anonymous basis.

Certain ITS applications (commercial vehicle operations or "mayday") require personally identifiable information to function. Others (such as automated fee payment) may be designed to enable use by individuals without identifying themselves (through anonymous debit accounts) or with identifiers for convenience (credit cards). Unless provision of identifiers is required by the ITS application, users should be provided with the opportunity to choose anonymity.

8. COMMERCIAL OR OTHER SECONDARY USE. Intelligent Transportation Systems information stripped of personal identifiers may be used for non-ITS applications.

American consumers want information used to create economic choice and value, but also want their interest in privacy preserved. ITS information is predictive of goods and services that interest consumers, for example, the right location for stores, hospitals and other facilities. However, personally identifiable

information collected by ITS surveillance technologies is extremely sensitive. Therefore, the following practices should be followed:

- ITS information absent personal identifiers may be used for ITS and other purposes.
- Generally, data collectors should assure that ITS information provided to private organizations for secondary uses is stripped of personal identifiers.
- Individuals, however, may contract to allow use of personal identifiers for secondary use if full disclosure in the intended use is made and informed consent obtained.

9. FOIA. Federal and State Freedom of Information Act (FOIA) obligations require disclosure of information from government maintained databases. Database arrangements should balance the individual's interest in privacy and the public's right to know.

In determining whether to disclose ITS information, governments should, where possible, balance the individual's right to privacy against the preservation of the basic purpose of the Freedom of Information laws to open agency action to public scrutiny. ITS travelers should be presumed to have reasonable expectations of privacy for personal identifying information. Pursuant to the individual's interest in privacy, the public/private framework of organizations collecting data should be structured to resolve problems of access created by FOIA.

10. OVERSIGHT. Jurisdictions and companies deploying and operating Intelligent Transportation Systems should have an oversight mechanism to ensure that such deployment and operation complies with their Fair Information and Privacy Principles.

Governments and companies should implement proper procedures to ensure that they protect the individual user's right to privacy, at a minimum, to the extent outlined in these principles. This mechanism may include internal directives, the appointment of a privacy officer, and/or penalties for violations. Governments and companies should have the flexibility to tailor such a system to their respective needs or circumstances.